

Strengthening the Nation's Core



Control Systems Security Center

A Department of Homeland Security program to secure national infrastructures

NATIONAL SECURITY

INL

Idaho National Laboratory

Threats to Control Systems

Many of the nation's critical infrastructures, such as oil and gas refineries, transportation systems, and telecommunication networks rely on sophisticated computer-based control systems to monitor and operate daily tasks. These automated systems collect data from the field, process and display this information for operators, and send control commands to local and remote equipment.

As identified by the Government Accountability Office, these control systems –

though efficient – are vulnerable to cyber intrusions by hackers, foreign intelligence services, and terrorist organizations.

Without proper security, intruders can potentially gain access to these critical systems compromising, disabling, and disrupting their essential functions.

DHS Response

The Department of Homeland Security has developed a strategy to quickly identify, prioritize, and respond to infrastructure vulnerabilities based on their impact to

public safety, security, and economic stability. As necessary, these vulnerabilities will be addressed directly, while technology and training will ensure effective solutions for future control systems.

Crucial to this strategy is the support that Idaho National Laboratory's Control Systems Security Center provides to DHS and the U.S. Computer Emergency Readiness Team.

The Center functions as a centralized location for industry, vendors, and government agencies to work

Continued on back

Continued from front

together to reduce cyber vulnerabilities in control systems. The facility and expert staff are capable of running mock exercises and calculated scenarios on full-scale control systems in a state-of-the-art research and testing facility.

Testing results are compiled and potential improvements are noted and sent to the equipment vendors for consideration. Additional efforts include industry outreach and awareness, vulnerability and risk assessments, analysis and tool development, and technical support for the U.S. CERT.

Employees of the Center represent a broad spectrum of talents and expertise in industry sectors such as oil and gas chemical, electric, telecommunications, and cyber security, among others. Their mission is to provide real solutions to the industry and vendors to help reduce and eliminate vulnerabilities in the control systems that operate our nation's critical infrastructures.

For more information:

Tom Harper
(208) 526-6566
Thomas.Harper@inl.gov

Jeff Hahn
(208) 526-6178
Jeffrey.Hahn@inl.gov
controlssecurity.inl.gov

A U.S. Department of Energy National Laboratory



The Control Systems Security Center is located at INL's Information Operation Research Center (IORC).



How it Works

The Center's control system experts gather field data, analyze existing systems for specific threats and vulnerabilities, and develop solutions to increase the defensive posture of critical infrastructure operating systems.

Employees perform vulnerability assessments on all types of control systems and associated components in an operationally infrastructure environment. The Center's intent is to expedite the development of next-generation, cyber security enhanced control systems by providing customers with relevant data, research facilities, and a highly-trained, technical staff.

Technical solutions in the private sector are also leveraged to eliminate vulnerabilities. At the same time, the Center works closely with key national resources including other federal laboratories, industry experts, trade groups, academia and federal, state, and local governments.

The Center works to formulate an integrated national response to:

- Identify and reduce control system vulnerabilities
- Help industry identify sector needs and security objectives
- Share sanitized information to facilitate improved designs
- Foster an environment for increasing awareness of control system cyber security

Awareness and Response

Plans are currently being developed to provide continuous support to the control systems division of the US-CERT. This role would allow experts from the Center to respond to emerging control system cyber security threats, work to prevent or limit the impact of cyber intrusions, and provide time-responsive analysis and solutions.

Industry Tools

Along with testing, evaluating, and performing analysis on control systems, the Center is developing security assurance levels for the control system industry and equipment vendors. Assurance levels provide a basis for improved security requirements based on the importance of each critical infrastructure and its potential for cascading effects on human health, environment, economy, and national security.

The Center is also creating a secure database to share information, research, and potential threats with the industry. The database will be validated and secure to protect specific stakeholder and national interests, and will provide information that has been sensitized of proprietary information.